REMARKS/ARGUMENTS

The Office Action has been carefully considered. It is respectfully submitted that the issues raised are traversed, being hereinafter addressed with reference to the relevant headings appearing in the Detailed Action section of the Office Action.

The Applicant has amended claims. The Applicant respectfully submits that the amendments to the claim set are fully supported by the originally filed specification.

Claim Rejections

The Examiner has maintained his rejections to claims 1 to 4, 6 to 15, and 17 to 20 under 35 U.S.C. 103(a) as being unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Spies *et al.* US Patent 6589565.

The Applicant is appreciative of the Examiner's detailed response to the Applicants previous submission. However, the Applicant respectfully disagrees with the Examiner's assertion that the present application is unpatentable over Sony in view of Spies.

The Examiner has rejected the present application as the Examiner believes that the claim limitation of "encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip", in claim 1, is shown in Sony and Spies. In particular, the Examiner has highlighted column 9 lines 31 to 48, column 9 line 57 to column 10 line 2, and Figure 9 of Sony.

In the Applicant's previous response, the Applicant highlighted to the Examiner that the Applicant fails to see any description, teaching or suggestion in the combination of Sony and Spies of the elements of claim 1, such as:

> 1. comparing the signature calculated in the trusted authentication chip with the decrypted signature;
> 2. in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip;

The Examiner seems to have rejected claim 1 as the Examiner believes that the use of signatures is shown in Spies, and the method of encrypting and decrypting random numbers is shown in Sony. The Applicant respectfully submits that in accordance with MPEP 2143, and in particular in the case of *In re Rouffet*, the Examiner's assertion is incorrect.

In particular, in the case of *In re Rouffet* it was determined that almost all inventions are a combination of known elements and that if patents could be rejected by merely identifying each claim element found in the prior art, then examiners could use hindsight (that is, the claimed invention itself) to defeat the patentability of the claimed invention, and accordingly very few patents would be granted.

In the present case, the Applicant is not suggesting that each of the features of the present claim 1 is shown in the cited prior art. The Applicant is only stating that the Examiner believes that the features of claim 1 are shown in Sony and Spies, however, the Examiner has ignored the holistic nature of the claim.

That is, claim 1 requires comparing the signature calculated in the untrusted authentication chip with the decrypted signature, and in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip.

The Examiner believes that Figure 9 of Sony shows encrypted random numbers RA and RB being passed from the R/W to the IC Card. However, there is nothing in Sony to suggest that there is a condition in place that needs to be satisfied in order to pass the encrypted random numbers between the R/W and the IC Card. Furthermore, there is nothing in Sony to suggest that that there is a requirement to compare signatures in a trusted authentication chip, and in the event that they match, returning the encrypted random numbers to the trusted authentication chip.

Furthermore, Spies is entirely silent with respect to the use of random numbers and only describes the use of randomly selected keys (see column 9 lines 30 to 33). Accordingly, there is no suggestion or teaching in Sony or Spies to combine the teachings of Sony and Spies in the particular way to achieve the particular method of claim 1.

The Applicant respectfully reminds the Examiner that in accordance with the case of *In re Rouffet*, a claim must be viewed in its entirety. The combination of Sony and Spies does not teach or describe comparing the signatures and in the event that the signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip.

Thus, the Examiner has failed to provide a motivation of the person skilled in the art for combining Sony and Spies to achieve the particular claimed invention. The Examiner seems to have just picked the features of claim 1 in certain prior art, and at the same time ignored the holistic nature of the claims, without providing any motivation as to how a person skilled in the art would achieve the particular claimed invention.

Furthermore, the combination of Sony and Spies fails to teach or suggest the claim limitation of comparing the signatures and in the event that the signatures match, encrypting the decrypted random number and returning it to the trusted authentication chip. Accordingly, the Examiner has failed to prove a *prima facie* case of obviousness, in accordance with MPEP 2143.

In any event, due to the long prosecution history of this case and in order to achieve expedited allowance, the Applicant has amended the present claim 1 to include the features of claim 3. Accordingly, claim 3 has been cancelled from the application.

Thus, the amended claim 1 describes the trusted authentication chip having a random function to produce random numbers from a seed, and the function advancing after each successful validation, so that the next random number is produced from a new seed.

The Applicant notes that as stated in the previous Office Action, the Examiner believes that Sony describes the random function feature of claim 3. In particular, the Examiner has highlighted column 8 lines 12 to 15 of Sony as disclosing this feature.

In contrast to Sony, the present amended claim 1 requires that the trusted authentication chip has a random function to produce random numbers. However, as Sony describes a method for mutual authentication, the random number of Sony is generated in the untrusted

component (see column 8 lines 12 to 17 and column 9 lines 49 to 52). Accordingly, Sony only describes the control section 11 of the R/W 1 generating a 64-bit random number R_A and the control section 81 of the IC card 2 generating a random number R_B.

Furthermore, there is no further description in Sony, of how the random numbers are generated. In contrast to Sony, the present amended claim 1 describes using a random function to produce the random numbers from a seed, where the function advances after each successful validation so that the next random number is produced from a new seed. Notably, Spies is also entirely silent on this feature.

Thus, the amended claim 1 is patentable over Sony in view of Spies.

Notably, similar amendments have also been made in respect of claims 11 and 15.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections. The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

Applicant:

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762